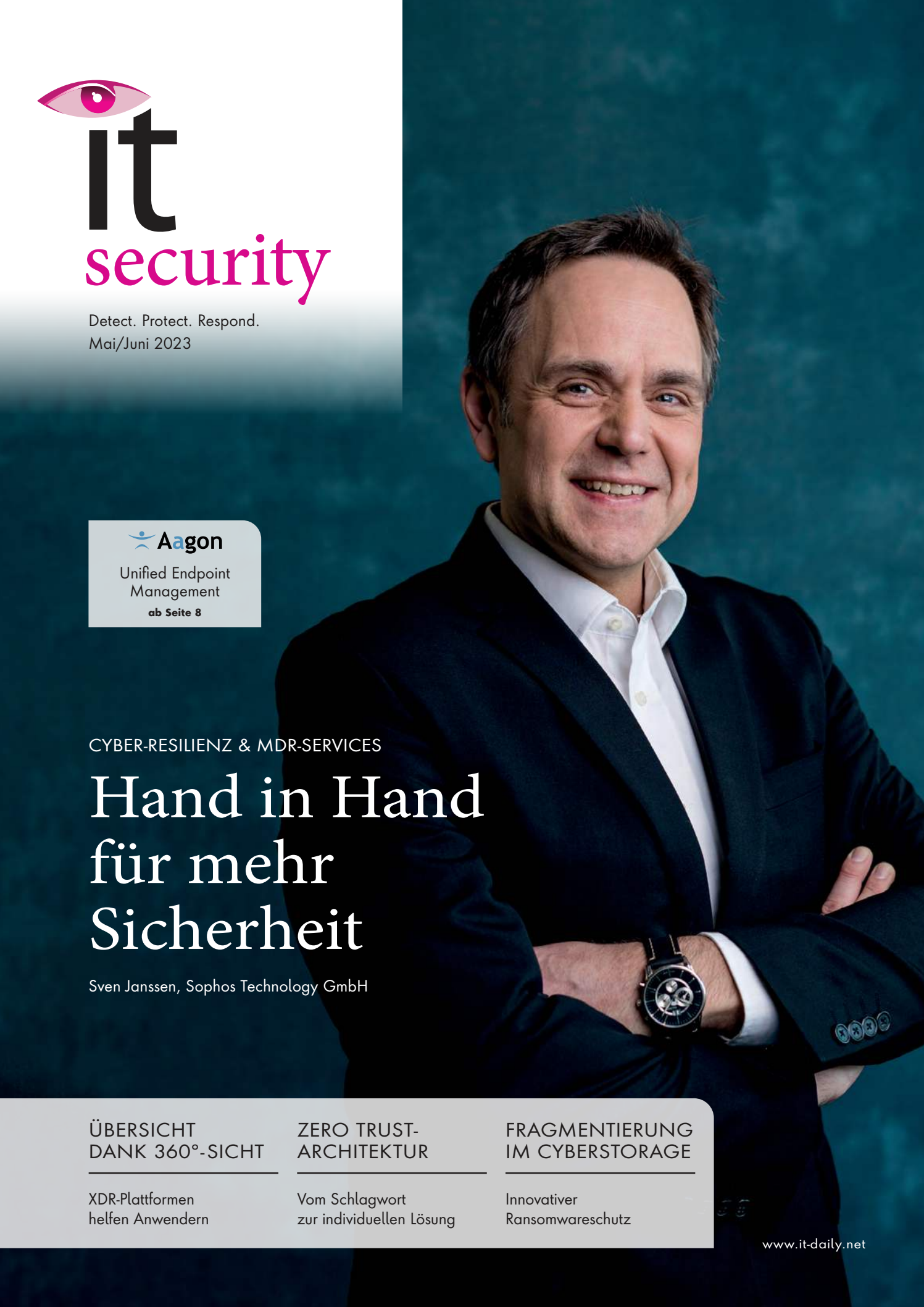
it security

Detect. Protect. Respond.
Mai/Juni 2023



Aagon
Unified Endpoint Management
ab Seite 8

CYBER-RESILIENZ & MDR-SERVICES

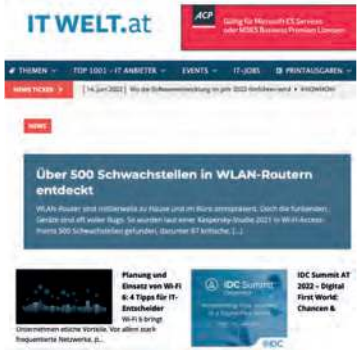
Hand in Hand für mehr Sicherheit

Sven Janssen, Sophos Technology GmbH

www.it-daily.net

IT WELT.at is IT

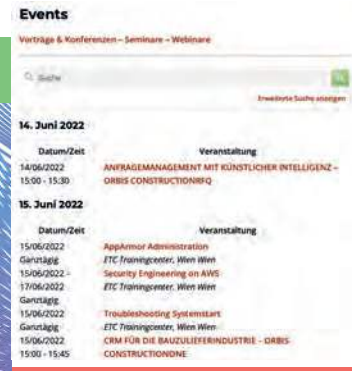
IT NEWS



Der tägliche Newsletter der ITWELT.at bringt die aktuellen IT Nachrichten aus Österreich und dem Rest der Welt. Wer immer up to date sein will, bestellt den kostenlosen Newsletter itwelt.at/newsletter und ist damit jeden Tag schon am Morgen am neuesten Informationsstand.

itwelt.at

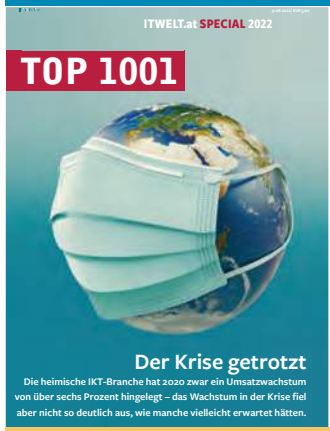
IT TERMINE



In Österreichs umfangreichster IT-Termindatenbank gibt es Termine für IT-Events wie Messen, Konferenzen, Roadshows, Seminare, Kurse und Vorträge. Über die Suchfunktion kann man Thema und Termin suchen und sich bei Bedarf auch gleich anmelden. Mit Terminkoordination und Erinnerung per E-Mail.

itwelt.at/events

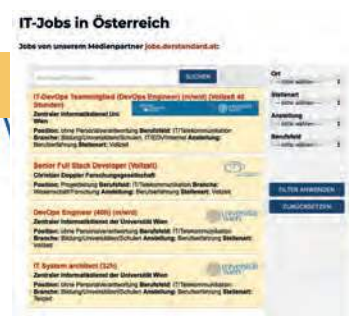
IT UNTERNEHMEN



TOP 1001 ist Österreichs größte IT-Firmendatenbank. Mit einer Rangliste der umsatzstärksten IT- und Telekommunikations-Unternehmen. Die Datenbank bietet einen Komplettüberblick der TOP IKT-Firmen und ermöglicht die gezielte Abfrage nach Tätigkeitsschwer-punkten, Produkten und Dienstleistungen.

itwelt.at/top-1001

IT JOBS



Hier sind laufend aktuelle IT Job-Angebote zu finden. In Zu-sammenarbeit mit der Standard.at/Karriere, dem Jobportal der Tageszeitung Der Standard, findet man auf dieser Plattform perma-nent hunderte offene Stellen aus dem Bereich IT und Telekom. Eine aktive Jobsuche nach Tätigkeits-feld und Ort ist natürlich möglich.

itwelt.at/jobs

Inhalt

COVERSTORY

IT SECURITY

Cyber-Resilienz und MDR-Services

HAND IN HAND FÜR MEHR SICHERHEIT

Cybersicherheit ist ein Thema, das uns gefühlt schon immer begleitet und das von Jahr zu Jahr wichtiger, aber auch komplexer wird. Durch die sich ständig verschärfende Bedrohungslage und das mittlerweile hoch professionelle Verhalten der Cyberkriminellen sind Unternehmen zu Sicherheitsstrategien angehalten, die auf einem weit höheren Level stattfinden als noch vor wenigen Jahren. Cyber-Resilienz ist ein wichtiges Stichwort und dazu gehört zusätzlich zur Software- und KI-gesteuerten Sicherheit auch eine menschliche Komponente in Form von Security-Services. Über die Managed Detection and Response (MDR)-Services sprechen Sven Janssen, Director Channel Sales DACH bei Sophos und Ulrich Parthier, Herausgeber it security.

Ulrich Parthier: *Wie kann man den heutigen Status der Cyberbedrohung kurz beschreiben und wie das Verhalten der Unternehmen?*

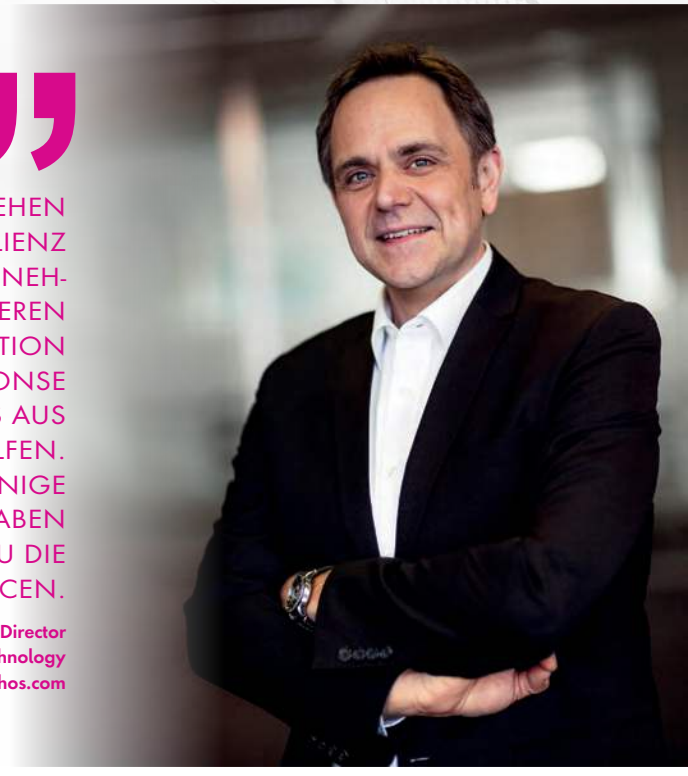
Sven Janssen: Die Landschaft der Cyberbedrohungen ist heute unglaublich vielfältig, wobei die Angriffstaktik über Ransomware nach wie vor und voraussichtlich auch in Zukunft den gefährlichsten Part einnimmt. Es ist nicht nur so, dass die Summen für die Lösegeldforderungen stetig steigen und dass die Akteure dahinter ihre Angriffe auf technisch höchstem Niveau durchführen. Die Cyberkriminellen haben zusätzlich zur Verschlüsselung der Daten den Datendiebstahl für sich entdeckt. Das hat zwei Gründe. Erstens sind viele Unternehmen mit ihrer Sicherheitsstrategie gegen Verschlüsselung heute besser gerüstet und verfügen über sichere Backups, was sie vor Lösegeldforderungen schützt. Der Datendiebstahl und der angedrohte Verkauf im Darknet ist jedoch für viele Unternehmen ein Grund, sich den Erpressern zu ergeben und zu bezahlen.

Auf der anderen Seite haben wir die Unternehmen, die sich deutlich bewusst sind, wie gefährlich das Internet ist. Allerdings hat eine unserer Studien ergeben, dass die Security immer noch nicht genügend in den Chefetagen angekommen ist, obwohl sie durchaus businesskritisch ist. Die große Mehrheit der befragten Manager (rund 81 Prozent) gab an, ein hohes bis sehr hohes Bewusstsein für IT-Sicherheit zu haben. Je größer die Unternehmen jedoch sind, desto weniger sieht sich die Führungsebene tatsächlich in der Verantwortung. Vor dem Hintergrund der aktuellen und neuen Regeln der Geschäftsführerhaftung ist das im Grunde fahrlässig.

Ulrich Parthier: *Cyber-Resilienz ist derzeit eines der Top-Themen. Was genau verstehen Sie darunter und wie setzt Sophos diesen Ansatz um?*

Sven Janssen: Zum einen ist Cyber-Resilienz die nächste höhere Stufe über

> WIR VERSTEHEN UNTER CYBER-RESILIENZ AUCH, UNTERNEHMEN MIT UNSEREN MANAGED DETECTION AND RESPONSE (MDR)-SERVICES AUS IHRER NOT ZU HELFEN. DENN NUR WENIGE UNTERNEHMEN HABEN DAZU DIE RESSOURCEN.
>
> **Sven Janssen, Senior Director Channel Sales, Sophos Technology GmbH, www.sophos.com**



der klassischen Security. Dabei geht es vor allem darum, eine noch höhere Erkennungssicherheit zu erreichen und auch die gezielten und trickreichen Angriffe abzuwehren. Die heute sehr guten technischen Lösungen aus vernetzten Security-Ökosystemen in Verbindung mit künstlicher Intelligenz werden daher mit menschlicher Expertise ergänzt. Denn Fakt ist, dass die technische Security zwar enorm viele Angriffe erkennen und abwehren kann. Für die letzten paar Prozent zur maximal möglichen Sicherheit benötigt man aber hoch spezialisierte Experten, die kontinuierlich die IT-Umgebung der Kunden beobachten und dabei die trickreichen Angriffe der besonders versierten Cyberkriminellen erkennen.

Zweitens verstehen wir unter Cyber-Resilienz auch, Unternehmen mit unseren Managed Detection and Response (MDR)-Services aus ihrer Not zu helfen. Denn nur wenige Unternehmen haben die Ressourcen, einen ganzen Stab an Security-Experten an Bord zu holen – ganz abgesehen davon, dass solche Experten schwer zu finden sind.

? **Ulrich Parthier:** *Und diese Experten sitzen bei Sophos und werden im Fall der Fälle selbstständig aktiv?*

Sven Janssen: Bei MDR-Services lagern Unternehmen den Sicherheitsbetrieb an externe Experten wie beispielsweise Sophos aus. Zu den Serviceleistungen gehören Analysen durch ein Expertenteam, Bedrohungssuche (Threat Hunting), Überwachung in Echtzeit sowie die Reaktion auf Vorfälle, kombiniert mit Technologien zum Erfassen und Analysieren von Bedrohungsdaten. Die Security Services werden je nach Vereinbarung mit dem Kunden auch selbstständig aktiv. Im Modus „Benachrichtigung" werden Kunden bei einer erkannten Bedrohung informiert und bekommen Detailinformationen, um eigene Teams bei der Priorisierung der potenziellen Gefahr zu unterstützen und die entsprechende Reaktion auszulösen. Im Modus „Zusammenarbeit" interagieren die Sophos-Experten mit den Ansprechpartnern, um auf erkannte Bedrohungen zu reagieren. In der dritten Variante kümmert sich das Sophos MDR-Team im Modus „Autorisierung" um alle erforderlichen Maßnahmen zur Eindämmung und Beseitigung von Bedrohungen inklusive der Information über die ergriffenen Maßnahmen. Diese Variante könnte man als Äquivalent für das individuelle Security Operations Center als umfassend gemanagter Service im Kampf gegen Cyberangriffe bezeichnen.

? **Ulrich Parthier:** *Ersetzen die MDR-Services ein klassisches SOC?*

Sven Janssen: Klassische Security Operations Center fand man in der Vergangenheit aufgrund der Komplexität und der hohen Kosten fast ausschließlich bei großen Unternehmen. MDR hat mit seinem Service-Konzept einen noch größeren Umfang und ist auch für KMUs in Reichweite. MDR-Services ersetzen also nicht nur das SOC, für viele Unternehmen macht es dieses Level an Sicherheit überhaupt erst möglich. Zudem greift ein MDR-Angebot nicht nur auf interne Datenquellen zu, sondern das Threat Hunting profitiert von einem riesigen Data Lake, der mit Daten aller Sophos-Kunden gefüttert wird. Das bietet ein riesiges Potenzial für effektive Bedrohungssuche.

? **Ulrich Parthier:** *Sie sprechen mit Reichweite die Kosten für MDR-Services an. Ist MDR wirklich günstiger und im Gegensatz zu einem SOC wirtschaftlich realisierbar?*

Sven Janssen: Unternehmen, die ihr eigenes SOC implementieren möchten, erkennen schnell, wie schwierig sich der Aufbau und vor allem der Betrieb gestaltet. Selbst in kleinen und mittelständischen Unternehmen würden mindestens vier Cybersecurity-Analysten benötigt, um ein SOC rund um die Uhr, jeden Tag im Jahr zu besetzen. Größere Unternehmen benötigen noch mehr teure Fachkräfte, die, wie gesagt, nur sehr schwer zu finden sind. Darüber hinaus braucht es Teamleiter und IT-Engineers zur Anpassung und Wartung von Tools. Zu diesen Personalkosten kommen weitere Kosten für Tools hinzu. Als Service entfällt ein großer Teil der genannten Personal- und Betriebskosten und ein Anbieter wie Sophos beziehungsweise die Partner können dies nicht nur aus wirtschaftlicher Sicht zu besseren Konditionen anbieten, sondern gleichzeitig mit einer weltweit vernetzten und damit wesentlich höheren Expertise.

? **Ulrich Parthier:** *Wie würden Sie in einem Elevator-Pitch die Vorteile von MDR-Services für Unternehmen beschreiben?*

Sven Janssen: Zusammengefasst gibt es fünf Gründe, weshalb Unternehmen zusätzlich zu einem technologie- und softwarebasierten Security-Ökosystem auch auf MDR-Services mit menschlicher Expertise setzen sollten: Die Härtung der Cyber-Abwehr, die Entlastung der verfügbaren IT-Ressourcen, das Hinzufügen von echter Expertise anstatt Headcount, die Optimierung des Return on Investments in die Cybersecurity und vor allem die Konzentration aller verfügbaren Ressourcen auf das Kerngeschäft.

! **Ulrich Parthier:** *Herr Janssen, herzlichen Dank für das Gespräch.*

Ein Schritt nach vorn für die Cybersicherheit?

GESETZE ZUR CYBER-RESILIENZ UND GESCHÄFTSFÜHRERHAFTUNG

Gesetze sind dafür da, Dinge klar zu regeln und im Idealfall sogar zu verbessern. Dazu gehören zu Recht Regeln zur Cybersicherheit, denn die Bedrohungslage wird seit Jahren zunehmend prekär und es entstehen große wirtschaftliche Schäden, sowohl für einzelne Unternehmen als auch aus volkswirtschaftlicher Perspektive. Zu den neuesten Gesetzen zählen das EU-weite Cyber-Resilienz-Gesetz sowie die Geschäftsführerhaftung bei Cyberangriffen.

Compliance-Anforderungen

Eine funktionierende und sichere IT ist für jedes Unternehmen von elementarer Bedeutung. Bei Cyberangriffen oder Verstößen gegen IT-sicherheitsrechtliche Vorschriften drohen dem Vorstand, der Geschäftsführung und/oder den Aufsichtsratsmitgliedern rechtliche Konsequenzen. Die Geschäftsleitung oder Aufsichtsratsmitglieder können zivilrechtlich auf Schadensersatz haften, wenn sie ihre Pflichten zur Sicherstellung der Digital Compliance vorsätzlich oder fahrlässig verletzen. Darüber hinaus können die Mitglieder der Geschäftsleitung und des Aufsichtsrats auch strafrechtlich belangt werden. Ein solcher Fall wäre denkbar, wenn aufgrund vorsätzlichen oder fahrlässigen Verhaltens durch einen Cybervorfall Geschäftsgeheimnisse oder Know-how des Unternehmens gegenüber unbefugten Dritten offenbart werden oder ein Angriff dazu führt, dass das Unternehmen seinen Geschäftsbetrieb vollständig einstellen muss und dadurch in die Insolvenz schlittert.

BEI IHREM RISIKOMANAGEMENT DÜRFEN DIE VERANTWORTLICHEN NICHT ALLEIN AUF TECHNISCHE MASSNAHMEN SETZEN, SONDERN MÜSSEN MENSCHLICHE EXPERTISE EINBINDEN.

Michael Veit, Security-Experte, Sophos Technology GmbH, www.sophos.com

Dem Unternehmen selbst können ebenfalls erhebliche Geldbußen drohen. Das Gesetz vom das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das vor allem die Betreiber „Kritischer Infrastrukturen", die Anbieter „Digitaler Dienste" und „Unternehmen im besonderen öffentlichen Interesse" betrifft, sieht Geldbußen in Höhe von bis zu 20 Millionen Euro vor. Nach der kürzlich verabschiedeten Richtlinie NIS 2.0 wird sich dieser Rahmen künftig weiter verschärfen. Die Richtlinie sieht Sanktionen in Höhe von zwei Prozent des weltweiten Jahresumsatzes vor. Noch drastischer können sich Verstöße gegen die datenschutzrechtlichen Vorschriften auswirken. Hier drohen Geldbußen von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes. Die neue EU Cybersecurity-Richtlinie NIS2 ist längst überfällig und wird dringend benötigt. Die Harmonisierung für die Einhaltung der Vorschriften in den einzelnen Mitgliedstaaten in Verbindung mit klar definierten Meldepflichten und Einhaltungsvorschriften sowie die Aktualisierung im Hinblick auf moderne Bedrohungen, sollten die Sicherheit und Stabilität der EU bezüglich disruptiver Angriffe erheblich verbessern. Die erweiterte Liste der Branchen ist zu begrüßen, lässt aber immer noch die Tür für nicht regulierte Unternehmen offen, die durch Angriffe auf die Lieferkette ein Risiko darstellen können.

EU Cyber-Resilienz-Gesetz

2022 hat die Europäische Union zudem einen Gesetzentwurf mit dem Titel „Cyber Resilience Law" vorgelegt. Darin wird ein horizontaler europäischer Ansatz zur Cybersicherheit befürwortet, der insbesondere Hardware- und Softwarehersteller betrifft, da diese die größte Verantwortung bei der Entwicklung (sicherer) technologischer Mittel tragen. Die Europäische Union hat große Ambitionen in Bezug auf dieses Cybersicherheitsgesetz. Sie glaubt zum Beispiel, dass sie durch klare Regeln für Technologiehersteller die Zahl der Cyberangriffe und damit die Gesamtkosten der Cyberkriminalität um 290 Milliarden Euro pro Jahr senken kann. Es steht die Frage im Raum: Wie realistisch sind diese Ambitionen?

Die Aufgabe besteht darin, die wichtigsten Engpässe im Bereich der Cybersicherheit zu ermitteln. Dabei sind jedoch strukturelle Herausforderungen zu meistern. Die erste ist das allgemeine Sicherheitsniveau der Technologie. Jedem vierten auf dem Markt befindlichen IKT-Produkt (Informations- und Kommunikationstechnologie) wird ein „niedriges" oder „sehr niedriges" Sicherheitsniveau attestiert. Einige Hersteller nehmen Abstriche bei der Sicherheit in Kauf, um ihre Produkte schneller auf den Markt zu bringen. Wenn das anfänglich niedrige Sicherheitsniveau später durch Updates korrigiert wird, geschieht dies meist, wenn eine Schwachstelle bereits entdeckt wurde. Das zweite strukturelle Problem ist der Mangel an Wissen über den verantwortungsvollen Umgang mit IKT-Produkten. In Europa geben sieben von zehn Nutzern zu, dass sie nicht ausreichend über die Risiken von Cyberangriffen informiert sind. Darüber hinaus betrachten die Endnutzer beim Kauf von Produkten die Sicherheit nicht als Hauptkriterium, weil sie zu oft annehmen, dass sie mit dem Design einhergeht.

Risikomanagement – Technik ist nicht genug

Bei ihrem Risikomanagement dürfen die Verantwortlichen – sprich Geschäftsleitung und Hersteller – nicht allein auf technische Maßnahmen setzen, sondern müssen menschliche Expertise einbinden. Denn viele Angriffe, bei denen sich die Hacker durch gestohlene Informationen Zugriff auf die Daten und Systemen ihrer Opfer verschaffen, verlaufen still und heimlich. Die Unternehmen stehen vor der Herausforderung, diese Angriffe bereits in der Entstehungsphase zu stoppen, noch bevor ein Schaden entstehen kann. Hierzu sind spezialisierte Bedrohungsexperten notwendig, die auf dem Arbeitsmarkt nur schwer zu finden sind und oft teuer eingekauft werden müssen. Die Folge: Zunehmend mehr Unternehmen entscheiden sich für Security-Services zusätzlich zu den technischen Security-Maßnahmen. Dazu zählen vornehmlich die MDR-Services (Managed Detection and Response), welche die eigene IT-Abteilung bei der Aufdeckung und Bekämpfung von Cyberangriffen unterstützt. Das ist nicht nur ein Trend. Denn laut Analysten von Gartner werden bis 2025 rund 50 Prozent aller Betriebe einen MDR-Service nutzen.

Um nachzuvollziehen, welche Vorteile ein MDR-Service bietet und was sich hinter der wachsenden Nachfrage verbirgt, ist es wichtig zu verstehen, was ein MDR-Service eigentlich ist – und was nicht. Managed Detection and Response (MDR) ist ein 24/7 Fully-Managed Service durch ein Team von Sicherheitsexperten, das darauf spezialisiert ist, Cyberangriffe zu erkennen und zu bekämpfen, die Technologielösungen allein nicht verhindern können. Die tägliche Cybersecurity-Verwaltung, wie die Bereitstellung von Sicherheitstechnologien, die Aktualisierung von Richtlinien oder die Installation von Updates, sind dagegen nicht Teil des MDR-Services. Managed Service Provider (MSPs) bieten entsprechende IT Security Management Services für Unternehmen und Einrichtungen, die Unterstützung in diesem Bereich benötigen.

Dass die Marktexperten von Gartner mit ihren Prognosen Recht haben, zeigt das große Interesse an Sophos MDR: Weltweit vertrauen bereits über 15.000 Unternehmen und Einrichtungen diesen Services. Und genau dieses Bewusstsein für das heutige und künftige Risiko im Cyberraum und das Engagement, die bestmögliche Security einzusetzen, wird Unternehmen und Hersteller gleich doppelt schützen: vor Cyberattacken auf das eigene Unternehmen und davor, mit den neuen Gesetzen zu Cyber-Resilienz und Geschäftsführerhaftung in Konflikt zu geraten.

Michael Veit

CHEFSACHE IT-SECURITY?

46,3 % sagen, dass die IT-Security seit mindestens zwei Jahren auf einer höheren Hierarchie angesiedelt ist

bei **39,8 %** der deutschen Unternehmen kümmert sich hauptsächlich die IT-Abteilung um die IT-Security

16,4 % der deutschen Unternehmen sehen IT-Security als Chefsache an

bei **33,8 %** der deutschen Unternehmen kümmert sich hauptsächlich ein Dienstleister um die IT-Security

(Quelle: Sophos)

Konsolidierung des Unified Endpoint Managements

DAS ZIEL HEISST: EINE EINHEITLICHE LÖSUNG!

Noch keine UEM-Lösung im Einsatz, Silolösungen oder Lösungen unterschiedlicher Hersteller in verschiedenen Werken und Tochtergesellschaften – das ist vielerorts noch business as usual. Über Lösungsansätze und Chancen sprach Ulrich Parthier, Herausgeber it management, mit Sebastian Weber, Head of Product Management bei Aagon.

Ulrich Parthier: *Picken wir uns exemplarisch einmal die Unternehmen heraus, die auf der grünen Wiese beginnen, also noch kein UEM im Einsatz haben. Wie gehen Sie hier vor? Gibt es ein Vorgehensmodell?*

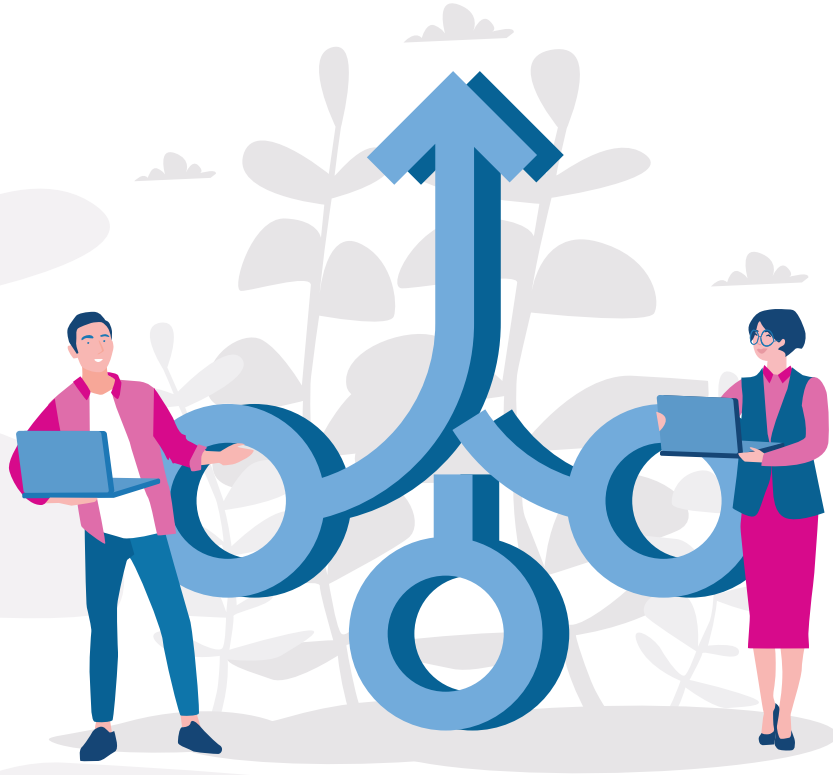
Sebastian Weber: Mittels Inventarisierung verschaffen wir uns zunächst einmal einen Überblick über die Client- und Serverlandschaft: Wie viele Arbeitsplätze gibt es, auf wieviel Standorte sind sie verteilt, welches Wachstum weist die IT-Landschaft auf? Ab etwa 50 Devices kann man damit rechnen, dass ein effizientes Reagieren auf Incidents nicht mehr zu bewältigen ist. Zusätzlich zur Arbeitserleichterung – Stichwort Turnschuh-Administration – geht es also heute in gleichen Teilen um Security.

Maßnahmen zur Vorsorge und Abwehr von Bedrohungen zu treffen, ist für kleine und mittelständische Unternehmen inzwischen obligatorisch, jedoch aufgrund des notwendigen Umfangs sehr personalintensiv oder nicht leistbar. Diese Maßnahmen lassen sich sehr gut mit einer UEM-Lösung wie der ACMP Suite umsetzen. Bei der Inventarisierung werden alle Clients in der Zentralkomponente erfasst, bei Aagon ist dies mit ACMP Core möglich. Anschließend kann es umstandslos mit den automatischen Updates und Patches losgehen; weitere Ausbaustufen wie OS Deployment, Lizenzverwaltung, Schwachstellenmanagement und ähnliches lassen sich schnell anschließen und erhöhen die Sicherheit der Infrastruktur.

Ulrich Parthier: *Unified Endpoint Management, warum ist es so wichtig, eine solche Lösung im Einsatz zu haben?*

Sebastian Weber: Kleine und mittelständische Unternehmen beschäftigen aus Kosten- und Kapazitätsgründen in der Regel nicht jeweils eigene Teams für Security, UEM oder Patching. Sie müssen alle Bereiche von Client Management und Security mit dünner Personaldecke bewältigen und suchen deshalb nach den besten Arbeitserleichterungen. Diese bieten ihnen UEM-Lösungen, denn damit können IT-Abteilungen alle Endgeräte im Netzwerk über eine zentrale Konsole verwalten und auf aktuellem Stand halten. Der wesentliche Punkt ist dabei, dass dies automatisiert stattfindet.

Die Automatisierung entlastet IT-Abteilungen nicht nur von aufwändigen manuellen Wartungsaufgaben, sie ermöglicht auch das Erreichen eines deutlich höheren Sicherheitsniveaus im Unternehmen. Denn neben Inventarisierung, Asset-, Update- und Patch Management gehört heute eben auch das Schwachstellen (Vulnerability)-Management zu den festen Modulen einer UEM-Lösung. In Anbetracht von Zero-Day-Exploits und ähnlichen Attacken ist es schlichtweg nicht mehr möglich, bei neuen Schwachstellen manuell angemessen gegenzusteuern. Erst Automatisierung garantiert bestmöglichen Schutz, weil dadurch ein jederzeitiger, aktueller Überblick über die Client-Landschaft gegeben ist.



Ulrich Parthier: *Wenn die Anforderungsphase abgeschlossen ist, also beispielsweise welche Geräte sollen unterstützt werden, welche Funktionen benötigen sie, welche Sicherheitsanforderungen müssen erfüllt werden, wie sieht es mit Integrationen, Skalierbarkeit und Support aus, dann stellt sich die Frage: welches ist das richtige Tool? Es gibt eine Vielzahl von UEM-Lösungen auf dem Markt. Helfen hier Checklisten weiter?*

Sebastian Weber: Aus unserer Marktbeobachtung heraus scheuen es Unternehmen, für verschiedene Einsatzzwecke jeweils spezielle Tools verschiedener Hersteller einzusetzen. Dagegen sprechen Kostengründe sowie auch die Handhabbarkeit. Bei Aagon setzen wir deshalb auf einen integrierten Ansatz. Dabei stehen alle Funktionalitäten im Zusammenhang mit Endpoint Management und IT-Security innerhalb einer Konsole bereit und werden darin verknüpft: Softwareverteilung, OS Deployment, Patch- und Schwachstellenmanagement und weitere. Der User kann sie je nach Bedarf lizenzieren und damit aktivieren.

Ulrich Parthier: *Automatisierung zum gebündelten Abarbeiten von Sicherheitsmaßnahmen läuft seit einiger Zeit unter dem Schlagwort Security Orchestration, Automation and Response, kurz SOAR. Können Unternehmen mit einer UEM-Lösung also SOAR umsetzen?*

Sebastian Weber: Beim SOAR-Konzept geht es um nichts anderes als um eine Sammlung von Funktionen, die darauf abzielen, durch Standardisierung und Priorisierung automatisiert und damit effizient auf erkannte Bedrohungen zu reagieren. Die drei grundlegenden SOAR-Bausteine für Sicherheits-Teams sind: Case- und Workflow-Management, Aufgabenautomatisierung sowie eine zentrale Methode, um Bedrohungsinformationen (die so genannte Threat Intelligence) aufzurufen, zu durchsuchen und zu teilen.

Jedes KMU, das seine Endpoints bereits über eine UEM-Plattform administriert, hat also im Prinzip schon alle Zutaten beisammen, die es zur Umsetzung von SOAR benötigt. Über eine einheitliche Konsole lässt sich SOAR daher im Mittelstand unkompliziert anwenden. Das funktioniert wie erläutert über die Verknüpfung der einzelnen Module: Aus dem Schwachstellenmanagement lässt sich mit wenigen Klicks ein Prozess erstellen, der bestimmt, dass ein Patch zur Fehlerbehebung eingespielt wird.

Ulrich Parthier: *Als Gründe, warum noch kein UEM im Einsatz ist, werden oft die Kosten und das fehlende Know-how von Mitarbeitern genannt. Sind diese Gründe nur vorgeschoben, und wie kann man sie gegebenenfalls entkräften?*

Sebastian Weber: Sobald die Fachkräfte in der IT-Administration erkannt haben, wie viel Zeit sie durch Einsatz einer UEM-Lösung sparen können, muss man eigentlich niemanden mehr groß überzeugen. Ihnen bleibt dadurch wesentlich mehr Freiraum für strategische Aufgaben, die sich nicht rein manuell erledigen lassen. Und mit dem schnellen ROI einer UEM-Lösung rennt man auch im Management offene Türen ein. Natürlich spielt die einfache Bedienung einer Konsole eine wesentliche Rolle bei der Akzeptanz – ganz unbenommen davon, dass in IT-Abteilungen technisches Know-how ja ohnehin selbstverständlich sein dürfte.

Ulrich Parthier: *Nun wird die IT ja immer komplexer, Stichwort On-Premises, Cloud, Managed Services. Was raten Sie hier den Unternehmen?*

Sebastian Weber: Wir haben es mit einer Komplexitätszunahme in zweierlei Hinsicht zu tun: Nicht nur die Security-Herausforderungen, auch übliche bekannte IT-Herausforderungen nehmen zu, weil die meisten Unternehmen heute in hybriden Umgebungen arbei-

ten, das heißt, sie sind sowohl On-Premises als auch in der Cloud unterwegs.

In hybriden Umgebungen kommen zu den herkömmlichen Clients noch einmal viele weitere Assets hinzu, die gleichwertig geschützt werden müssen: Ladesäulen, Zutrittskontrollen, IoT-Devices, Temperatursensoren in der OT. Sie alle stellen Angriffsflächen dar; gleichzeitig werden die Attacken immer raffinierter und intelligenter. Dies zusammengenommen spricht gerade für UEM, denn Unternehmen stehen vor der Aufgabe, cloud-basierte und inhouse installierte Security-Lösungen unter ein Dach zu bringen und zentral zu managen. Genau hier kann UEM umfassend unterstützen.

Ulrich Parthier: *Als Ersatz für eine vollintegrierte Lösung müssen oft Teillösungen herhalten, die bereits tief im Betriebssystem integriert sind – wie Microsoft Defender und BitLocker. Das kostet nichts und wiegt die Unternehmen in Sicherheit. Ist das eine gefährliche Strategie?*

Sebastian Weber: Ganz im Gegenteil! Microsoft hat in den letzten Jahren große Anstrengungen unternommen, seine Security-Lösungen Defender und Bitlocker zu verbessern, und dies nicht ohne Erfolg: Inzwischen sind die Redmonder Leader im Gartner Magic Quadrant for Endpoint Protection Platforms. Dass die Grundfunktionen bereits tief im Betriebssystem verankert sind, bedeutet zudem keine hohen zusätzlichen Kosten. Da die Anwenderoberfläche des Defenders, als auch BitLockers, in der Vergangenheit nicht gerade mit Benutzerfreundlichkeit geglänzt hat, hat Aagon die Module ACMP Defender Management und ACMP BitLocker Management entwickelt. Sie versetzen Administrations-Abteilungen in die Lage, die Microsoft Lösungen in nur einer Oberfläche auf allen Clients und Servern zu verwalten.

DIE AUTOMATISIERUNG ENTLASTET IT-ABTEILUNGEN NICHT NUR VON AUFWÄNDIGEN MANUELLEN WARTUNGSAUFGABEN, SIE ERMÖGLICHT AUCH DAS ERREICHEN EINES DEUTLICH HÖHEREN SICHERHEITSNIVEAUS IM UNTERNEHMEN.

Sebastian Weber,
Head of Product Management, Aagon,
www.aagon.com

Ulrich Parthier: *Funktionen und Integrationen bei UEM-Plattformen sind essentiell. Es ist ja extrem komplex, geht es doch um Gerätemanagement, Anwendungsmanagement, Datenmanagement, Identitätsmanagement und natürlich um Integrationsmöglichkeiten. Wie sehen Sie bei Aagon das Szenario?*

Sebastian Weber: Aufgrund unserer langjährigen Erfahrung im UEM-Bereich verknüpfen wir die verschiedenen Funktionalitäten wie bereits beschrieben miteinander. Aufbauend auf dem notwendigen Fundament der Inventardaten und der daraus gewonnenen Erkenntnisse entsteht die Möglichkeit des integrierten und automatisierten Security-Managements.

Ulrich Parthier: *Abschließend die Frage, wie es mit dem Reporting, der Compliance und den Auditing-Funktionen aussieht. Sind die in der Lösung bereits enthalten?*

Sebastian Weber: Eine Reporting-Funktion in unserer UEM-Konsole liefert zeitlich automatisch einstellbare Statusinformationen. In einem frei konfigurierbaren Dashboard kann die IT-Administration zusammenstellen, was im SOAR-Kontext angezeigt werden soll: Daten aus der CVE-Datenbank (Wo befinden sich die meisten betroffenen Rechner?), aktueller Patch-Stand, Auswertung des Defender (gibt es gerade besonders viele Ereignisse, auf die er reagiert hat?) etc. Auf diese Weise können auch mittelständische Unternehmen mit kleinerem IT-Budget ein zeitgemäßes SOAR-Konzept zur Sicherung ihres Netzwerkbetriebs aufsetzen.

Ulrich Parthier: *Herr Weber, wir danken für das Gespräch!*

THANK YOU